

REMARKS

Applicant acknowledges with appreciation that Claims 6, 15, 28, 32, 35, 40, 45, 49, 64 and 80 are allowable if rewritten in independent form. New claims 85-89 are added.

Claims 7, 33, 36, 38, 46 and 77 were rejected under 35 U.S.C. 112 as being indefinite. Claims 7, 33, 36, 38, 46 and 77 are herein amended to address the issues raised in the Office Action.

Specifically, Claims 7, 36 and 46 are amended to recite the part specifying means specifies the certain part in the content data by performing, in the order specified by the cryptographic information, operations indicated by each of the instructions (Figures 2, 3 and 5 and Specification page 38 ll. 15-21 and page 39 line 20 to page 40 line 1). Each of the instructions is read, interpreted, and executed in turn. Applicant notes that the bit data detected by the detect instruction in Claim 7 and others does not affect the order in which the reference and detect instructions are performed. The cryptographic information simply includes information which indicates the order in which operations instructed by the reference instruction and the detect instruction are performed (Specification page 11 ll. 11-14). In this way, the cryptographic information determines an order in which a bit data is detected first according to the detect instruction and then an operation is executed according to the reference instruction which references a data section at a position relative to the detected position (Specification page 36 ll. 6-11).

Claim 33 is amended to recite the cryptographic information further includes flag pattern information showing a bit sequence, which is not the certain bit sequence shown by the sync pattern information, and position information specifying the position of the bit sequence (Figures

18-19 and Specification page 74 line 19 to page 75 line 6, page 77 ll. 11-15, page 78 ll. 12-19). Applicant notes that the bit sequence relates to the flag pattern information (Specification page 79 ll. 10-21).

Claim 38 is amended to recite the cryptographic processing means performs one of encryption and decryption on the certain part using the specified algorithm, as understood in the Office Action (Figures 2, 7, and 21 and Specification page 36 ll. 10-15 and page 81 ll. 2-11).

Claim 77 is amended to recite the cryptographic information further includes a detect instruction for detecting, from the content data, bit data that matches the certain bit sequence shown by the bit pattern information, and specifies the order in which the reference and detect instructions are performed (Figures 3 and 5 and Specification page 34 ll. 3-15).

Applicant respectfully requests this rejection be withdrawn.

Claims 42-44, 47-48, 66-69 and 84 were rejected under 35 U.S.C. 102(b) as being anticipated by *Yorke-Smith* ("Yorke" U.S. Patent No. 5,548,648).

The present invention, as defined in the claims, is drawn to a general purpose cryptographic apparatus for performing cryptographic processing on content data that is specified by searching for and referring to a data section of the content data as indicated by a reference instruction (Specification page 7 ll. 1-7 and page 18 ll. 1-14). In this manner, the present invention eliminates the problem of needing to store information in the cryptographic apparatus in advance for specifying the part of the content data upon which cryptographic processing is to be performed (Specification page 8 ll. 3-12).

In contrast, the Yorke reference is drawn to an encryption method and system that makes use of multiple encryption techniques for the same data set in order to make unauthorized decryption very difficult, and an associated control block comprising an indication of the encryption functions used to encrypt the data (Yorke col. 1 ll. 48-65). The Yorke reference teaches using the control block to determine the encryption functions and does not teach searching for or referring to a specific data section in the content data as identified by a reference instruction.

Claims 42, 66, and 84 are amended to recite a part specifying means or step for specifying the certain part of the content data based on the cryptographic information by searching for and referring to the data section in the content data as indicated by the reference instruction (Figures 2, 5 and 7 and Specification pages 40 ll. 9-18, 44 ll. 2-5, 50 ll. 4-10 and 52 ll. 11-15). Claims 42, 66, and 84 clearly identify the part specifying means and the part specifying steps specify by searching for a specific data section in the content data for the certain part upon which the cryptographic processing is to be performed. The searching process is illustrated in part by the looping function after obtaining the cryptographic information (Figures 5 and 7 and Specification page 39 line 15 to page 40 line 8). Once the position of the detected header is found, for example, the position is used as a reference point. By this claim amendment it becomes clear that the part specifying means (steps) identify the certain part on which the cryptographic processing is to be performed by "searching" for a specific data section in the content data. In this way, the certain part of content data in various formats can be specified by the position of the searched specific data section that is relative to the position of the certain part. In the section AMENDMENTS TO THE SPECIFICATION the paragraph on page 18 ll. 1-14 is amended to provide literal support for the phrase "searching for".

The Yorke reference teaches a technique for specifying an encrypted data segment, on which a cryptographic processing is to be performed according to the indication for the starting position (S) of the encrypted data segment within the control block regardless of the data content of the encrypted data block (Yorke Figures 4 and 6 elements 470 and 620 and col. 4 ll. 33-37 and col. 5 ll. 31-35). Applicant respectfully submits that the only relevant description within the Yorke reference regarding the data content of the encrypted data block is "... the invention is not limited to a fixed length encrypted data block and the code above can be readily modified to implement an embodiment having a variable length encrypted data block" (Yorke col. 9 ll 15-26). Applicant respectfully submits this description in Yorke does not teach searching for and referring to the data section in the content data based on a reference instruction, as presently claimed.

Claims 43-44 and 47-48 depend either directly or indirectly from Claim 42 and are believed allowable based on the allowance of Claim 42, as amended. Similarly, Claims 67-69 depend either directly or indirectly from Claim 66 and are believed allowable based on the allowance of Claim 66, as amended. Applicant respectfully requests this rejection be withdrawn.

Claims 1-5, 8-14, 16-17, 70-76 and 78-79 were rejected under 35 U.S.C. 103(a) as being unpatentable over Yorke in view of *Glover* ("Glover" U.S. Patent No. 6,052,780).

Glover is drawn to allowing a content provider to encrypt information without requiring either a hardware or platform manufacturer or a content consumer to provide support for the specific form of corresponding decryption and allows the content to be copied and transferred without permitting copying of the content in decrypted form (*Glover* col. 3 ll. 37-46). The encrypted content is stored as an executable program that includes a decryption program that decrypts the encrypted content when a user successfully completes an authorization procedure

(Glover col. 3 ll. 47-51). Glover teaches computer program "logic" stored on a computer readable medium that defines several modules where the modules provide executable code for decrypting the other modules (Glover col. 5 ll. 4-20). Glover does not teach searching for and referring to the data section in the content data based on a reference instruction, as presently claimed.

In reference to Claim 42 above, Claim 1 is similarly amended to recite the part specifying means for specifying the certain part of the read content data at least by searching for a specific data section in the read content data (Figures 2, 5 and 7 and Specification pages 22 ll. 14-19, 40 ll. 9-18, 44 ll. 2-5, 50 ll. 4-10 and 52 ll. 11-15). Claim 1, as amended, identifies the certain part is specified by at least making a search of the content data. In one instance, a predetermined bit pattern in the content data is searched for, and a part which is at a predetermined position relative to the position of the searched bit pattern can be specified as the certain part. Applicant notes that the search includes processing such as collating data in the content data with the predetermined bit pattern. In this case, if the predetermined bit pattern is at a proper position relative to the position of the certain part, content data in any format can be handled similarly, and the certain part of the content data in any format can be specified. In the section AMENDMENTS TO THE SPECIFICATION the paragraph on page 22 ll. 14-19 is amended to provide literal support for the phrase "a specific data section".

As noted in the Office Action, Glover teaches encrypting and distributing content on portable media. However, neither Yorke nor Glover teach or suggest searching for a specific data section in the content data, as presently claimed. Applicant respectfully submits that even if the references are combined as suggested that they do not teach all of the claimed elements, and therefore cannot be used to render the present invention obvious. Similarly, Claims 2-5, 8-14,

and 16-17 depend directly or indirectly from Claim 1 and are believed allowable based on the allowability of Claim 1, as amended.

In reference to Claim 1, Claim 70 is similarly amended to recite a cryptographic information recording area in which cryptographic information, including information used to specify the certain part of the content data by searching for a specific data section in the content data (Figures 2, 5 and 7 and Specification pages 22 ll. 14-19, 40 ll. 9-18, 44 ll. 2-5, 50 ll. 4-10 and 52 ll. 11-15). As noted in the Office Action, Glover teaches a portable media. However, neither Yorke nor Glover teach searching for a specific data section in the content data, as presently claimed. Applicant respectfully submits that even if the references are combined as suggested that they do not teach all of the claimed elements, and therefore cannot be used to render the present invention obvious. Similarly, Claims 71-76 and 78-79 depend directly or indirectly from Claim 70 and are believe allowable based on the allowance of Claim 70, as amended. Applicant respectfully requests this rejection be withdrawn.

Claims 18, 58-59 and 82 were rejected under 35 U.S.C. 103(a) as being unpatentable over Yorke in view of Glover, as applied to Claim 17, and in further view of *Kelly* ("Kelly" U.S. Patent No. 5,475,757).

Kelly teaches a secure data transfer method that includes a challenge from a subscriber along with secret information to form a subscriber's response and avoids the need to prior knowledge at either of the transmission ends of any coding key being used at the other end (Kelly col. 2 ll. 43-52, col. 4. ll. 17-33, and Abstract). Kelly teaches another unit receives this challenge and decrypts the encrypted transmission (Kelly col. 4 ll. 34-59). Kelly is addressing a very different issue, and cannot be combined to teach searching for a specific data section in the content data, as presently claimed.

Similar to Claim 1, Claims 58 and 82 are amended to recite a part specifying step for specifying the certain part of the content data based on the read cryptographic information at least by searching for a specific data section in the content data (Figures 2, 5 and 7 and Specification pages 22 ll. 14-19, 40 ll. 9-18, 44 ll. 2-5, 50 ll. 4-10 and 52 ll. 11-15).

As mentioned in the Office Action, Kelly teaches that when an intermediary is involved in a transmission, a message is decrypted and then re-encrypted using the same algorithm. However, neither Yorke nor Kelly teach or suggest searching for a specific data section in the content data, as presently claimed. Applicant respectfully submits that even if the references are combined as suggested that they do not teach all of the claimed elements, and therefore cannot be used to render the present invention obvious. Similarly, Claim 59 depends from Claim 58 and is believed allowable based on the allowance of Claim 58. Applicant respectfully requests this rejection be withdrawn.

Claims 19-27, 51-57, 60-61 and 81 were rejected under 35 U.S.C. 103(a) as being unpatentable over Yorke in view of Glover, in further view of Kelly.

In reference to Claims 1 and 58, Claims 19, 51, and 81 are similarly amended to recite the part specifying means for specifying the certain part of the obtained content data based on the read cryptographic information at least by searching for a specific data section in the obtained content data (Figures 2, 5 and 7 and Specification pages 22 ll. 14-19, 40 ll. 9-18, 44 ll. 2-5, 50 ll. 4-10 and 52 ll. 11-15). However, none of Yorke, Glover, or Kelly teach or suggest searching for a specific data section in the content data, as presently claimed. Applicant respectfully submits that even if the references are combined as suggested that they do not teach all of the claimed elements, and therefore cannot be used to render the presently claimed invention obvious. Similarly, Claims 20-27 depend directly or indirectly from Claim 19 and are believed allowable

based on the allowance of Claim 19, as amended. Claims 52-57 depend from Claim 51 and are believed allowable based on the allowance of Claim 51. Finally, Claims 60-61 depend from Claim 58 and are believed allowable based on the allowance of Claim 58, as amended and discussed above. Applicant respectfully requests this rejection be withdrawn.

Claims 29-31, 34, 37-39, 41, 50, 62-63, 65 and 83 were rejected under 35 U.S.C. 103(a) as being unpatentable over Yorke in view of *Cornaby et al.* ("Cornaby" U.S. Patent No. 5,875,349).

Cornaby teaches a communication method between a computer and a data storage device that requires certain device operating data/code in the form of device control means and device operating data to be used in control of the operation of the device (Cornaby col. 9 ll. 40-50). Cornaby is drawn to reducing the cost and complexity of the storage device by allowing the operating data and code to be stored in system RAM (Cornaby col. 9 ll. 23-32). Cornaby does not teach specifying the certain part of the content data by searching for and referring to a specific data section, as presently claimed.

In reference to Claims 1 and 42, Claims 29, 62 and 83 are amended to recite a part specifying means for specifying the certain part of the obtained content data based on the obtained cryptographic information at least by searching for a specific data section in the obtained content data (Figures 2, 5 and 7 and Specification pages 22 ll. 14-19, 40 ll. 9-18, 44 ll. 2-5, 50 ll. 4-10 and 52 ll. 11-15).

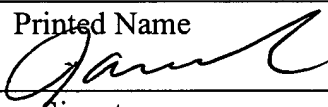
As noted in the Office Action, Cornaby teaches an arrangement for allowing a computer to communicate with a storage device over a bus, such as a multiplexed bus (Cornaby col. 11 ll. 64-67 and col. 12 ll. 1-16). However, neither Yorke nor Cornaby teach or suggest searching for a specific data section in the content data, as presently claimed. Applicant respectfully submits

that even if the references are combined as suggested that they do not teach all of the claimed elements, and therefore cannot be used to render the present invention obvious. Claims 30-31, 34, 37-39, 41 depend directly or indirectly from Claim 29 and are believed allowable based on the allowance of Claim 29, as amended. Claim 50 depends directly from Claim 42 and is believed allowable based on the allowance of Claim 42, as amended. Finally, Claims 63 and 65 depend directly from Claim 62 and are believed allowable based on the allowance of Claim 62, as amended. Applicant respectfully requests this rejection be withdrawn.

New Claims 85-89 are believed allowable based on the allowance of the original Claims 15, 28, 40, 49 and 80 as rewritten in independent form. Specifically, Claim 85 is the original Claim 15 as rewritten in independent form and as dependent from Claims 1, 13 and 14. Claim 86 is the original Claim 28 in independent form and as dependent from Claims 19, 26 and 27. Claim 87 is the original Claim 40 in independent form and as dependent from Claims 29, 38 and 39. Claim 88 is the original Claim 49 in independent form and as dependent from Claims 42, 47 and 48. Claim 89 is the original Claim 80 in independent form and as dependent from Claims 70, 78 and 79.

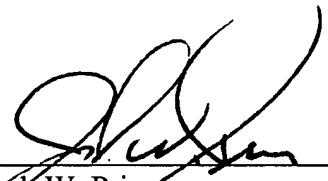
It is believed that the case is now in condition for allowance, and an early notification of the same is requested. If the Examiner believes that a telephone interview will help further the prosecution of this case, he is respectfully requested to contact the undersigned attorney at the listed telephone number.

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on July 23, 2004:

Date: July 23, 2004
By: James Lee
Printed Name

Signature

Respectfully submitted,

SNELL & WILMER L.L.P.



Joseph W. Price
Registration No. 25,124
1920 Main Street, Suite 1200
Irvine, California 92614-7230
Telephone: (949) 253-4920
Facsimile: (949) 955-2507